

What Is Claimed Is:

1 1. A method for remotely configuring a device across a network,
2 comprising:
3 receiving configuration information at the device from a remote system
4 across the network;
5 encrypting the configuration information using a device key, wherein the
6 device key is locally stored at the device and is different from keys associated
7 with other devices; and
8 configuring the device by storing the encrypted configuration information
9 in a non-volatile configuration store associated with the device;
10 whereby the encrypted configuration information contained in the non-
11 volatile configuration store cannot be used with another device.

1 2. The method of claim 1, wherein receiving the configuration
2 information involves using a secret key, which is locally stored at the device, to
3 decrypt the configuration information received from the remote system.

1 3. The method of claim 1, wherein receiving the configuration
2 information involves using a public key of the remote system to validate that the
3 configuration information was digitally signed by a corresponding private key
4 belonging to the remote system.

1 4. The method of claim 1, wherein the device key is stored in one-
2 time programmable memory within the device that can be programmed only once
3 and cannot be reprogrammed.

093262 053464
F07E0 2992280

1 11. An apparatus that facilitates remotely configuring a device across a
2 network, comprising:
3 an interface, at the device, that is configured to receive configuration
4 information from a remote system across the network;
5 an encryption mechanism that is configured to encrypt the configuration
6 information using a device key, wherein the device key is locally stored at the
7 device and is different from keys associated with other devices; and
8 a configuration mechanism that is configured to store the encrypted
9 configuration information in a non-volatile configuration store associated with the
10 device;
11 whereby the encrypted configuration information contained in the non-
12 volatile configuration store cannot be used with another device.

1 12. The apparatus of claim 11, further comprising a decryption
2 mechanism that is configured to use a secret key, which is locally stored at the
3 device, to decrypt the configuration information received from the remote system
4 through the interface.

1 13. The apparatus of claim 11, further comprising a validation
2 mechanism that is configured to use a public key of the remote system to validate
3 that the configuration information was digitally signed by a corresponding private
4 key belonging to the remote system.

1 14. The apparatus of claim 11, further comprising a one-time
2 programmable memory within the device for storing the device key;
3 wherein the one-time programmable memory can be programmed only
4 once and cannot be reprogrammed.

1 15. The apparatus of claim 11, further comprising a content screening
2 mechanism that is configured to use the configuration information to control
3 access to a stream of content in order to facilitate subscriber management.

1 16. The apparatus of claim 15, wherein the configuration information
2 includes either a fixed key or a variable key for decompression and/or decryption
3 of the stream of content.

1 17. The apparatus of claim 11, wherein the device includes one of:
2 a computer;
3 a personal digital assistant;
4 a network interface;
5 a cable television interface;
6 a satellite television interface; and
7 a network router.

1 18. The apparatus of claim 11, wherein the network includes one of:
2 a local area network;
3 a wide area network; and
4 a wireless network.

1 19. The apparatus of claim 11, wherein the configuration mechanism
2 can enable and/or disable the device.

1 20. The apparatus of claim 11, further comprising an integrated circuit
2 upon which the device is embodied.

1 21. The apparatus of claim 11, wherein the interface is configured to
2 support one-way communication from the remote system to the device.

1 22. The apparatus of claim 11, further comprising a local interface on
2 the device for communicating with local resources;
3 wherein the local interface is insulated from the configuration information
4 stored in the non-volatile configuration store, so that it is impossible to access the
5 configuration information through the local interface.

1 23. An apparatus that facilitates remotely configuring a device across a
2 network, comprising:
3 an interface, at the device, that is configured to receive configuration
4 information from a remote system across the network;
5 a decryption mechanism that is configured to use a secret key, which is
6 locally stored at the device, to decrypt the configuration information received
7 from the remote system through the interface;
8 an encryption mechanism that is configured to encrypt the configuration
9 information using a device key, wherein the device key is locally stored at the
10 device and is different from keys associated with other devices; and
11 a configuration mechanism that is configured to store the encrypted
12 configuration information in a non-volatile configuration store associated with the
13 device; and
14 a one-time programmable memory within the device for storing the device
15 key and the secret key, wherein the one-time programmable memory can be
16 programmed only once and cannot be reprogrammed;

17 whereby the encrypted configuration information contained in the non-
18 volatile configuration store cannot be used with another device.

1 24. The apparatus of claim 23, further comprising a content screening
2 mechanism that is configured to use the configuration information to control
3 access to a stream of content in order to facilitate subscriber management.

1 25. The apparatus of claim 23, further comprising a validation
2 mechanism that is configured to use a public key of the remote system to validate
3 that the configuration information was digitally signed by a corresponding private
4 key belonging to the remote system.